Methods and algorithms for analysis of behavior of fractal and chaotic components of cyclic trajectories of nonlinear congruent dynamical systems

Vostrov G. Krinenko A. Shcherbaniuk O.

Introduction

The current level of development of information theory creates the illusion that with the help of existing methods of its application it is possible to solve any problems of controlling complex dynamic systems of any level of complexity. This is facilitated by a sufficiently developed idea that applied problems and technologies for their solution do not largely depend on the level of development of the mathematical foundations of information theory, in fact, the number of "dark" spots in the theory of application of modern methods of information theory is only growing, because the actual discoveries in the study of the properties of their trajectories create more and more new questions, the answers to which humanity does not have now. The study of the world around us, attempts to control and manage its individual parts lead us to the conclusion that our life is a huge, in its volume, nonlinear dynamic stochastic system that randomly changes every moment. The systematic growth of interest in the qualitative, algorithmic, informational, structural properties of dynamical systems, depending on the initial conditions for the formation of their cyclic trajectories and the mathematical features of their nonlinear definition, necessitates the correct formulation of the problem and the definition of directions for its solution. In this regard, further development of the theory of dynamical systems is more relevant than ever[1].

The so-called "dark" spots include the problem of studying the structure of trajectories of cyclic fixed points of nonlinear dynamical systems depending on the initial conditions. In this case, first of all, it is necessary to mathematically substantiate to what extent the fractal and chaotic components of their trajectories and their distribution in cyclic trajectories depend on the properties of the initial conditions. According to the Sharkovsky's theorem [2] on the ordering of fixed points by the length of cyclic trajectories, it follows that any dynamical system having at least one cyclic fixed point with trajectory length three entails the existence of cyclic fixed points with any trajectory length in this dynamical system. In general, the statement determines that this leads to the creation of so-called chaos. At first glance, chaos cannot exist alongside the classical definition of dynamical systems, which assures that given initial conditions, one can unambiguously predict the behavior of the trajectory of a dynamical system. This point of view does not lead to contradiction. In the chaotic behavior of dynamical systems, the slightest inaccuracy in determining the initial state of the system leads to an increase in its influence on the behavior of the trajectory over time, and therefore forecasting becomes ineffective or almost impossible. Mastering chaos is becoming one of the most important problems of our time. The solution of this problem leads us to try to understand all the variety of nonlinear phenomena and processes that make up our life [3].

Due to the dynamic nature of chaotic modes and their sensitivity to the slightest fluctuations, they provide effective control by means of external controlled influence. The purpose of such influence can be the implementation of a periodic mode in the system instead of chaos or getting into a given region of phase space. This idea was first introduced and considered in works [4,5] and is quite promising in the theoretical and applied sense to this day.

Another direction of using the ideas and methods of nonlinear dynamics is related to the problem of signal processing[6]. Suppose that a remote and inaccessible object is studied, so the research possibilities are limited to the analysis of the signal coming from it. Over the past few decades, methods have been developed to find out whether this signal was created by a dynamic system, as well as to obtain information about the properties of this system. The development of methods and algorithms for signal analysis can be considered an important area of nonlinear dynamics directly related to further applications [7].

The aim of this work is to create mathematical foundations for the analysis of the behavior and structures of cyclic trajectories of complex dynamical systems as a way to determine the chaos in nonlinear stochastic dynamical systems of varying complexity. It is especially important to reveal the structure of chaotic processes of trajectories of cyclic fixed points over a large length, which are determined by numbers of the form 1/p, where p is a prime number. The analysis of such trajectories is important for the reason that the structures of trajectories for initial values of n/m, where n and m are composite numbers, may have completely different properties of cyclic trajectories of fixed points. In the first case, on the basis of number theory, it is possible to describe analytically the properties of trajectories defined by initial conditions with prime numbers using functional mappings created on the basis of group theory[8]. Entropy can be considered as a tool to measure the complexity of trajectories. Methods for calculating the difference between the entropy before the analysis of the structure of cyclic trajectories of fixed points and the entropy after the separation of its structure can be considered as a process of obtaining new information about chaos in cyclic trajectories of nonlinear dynamical systems[8,9,10].

Thus, it will be established whether the trajectories of cyclic fixed points actually create a group of permutations, whether the resulting trajectories have a deterministic structure, and how the choice of the initial state of the dynamical system affects the construction of these trajectories, in particular when working on a set of integers, rational or real numbers. In general, we can consider models of dynamical systems in complex space. Regardless of the choice of sets over which models of theoretical or applied dynamical systems are built, an important problem is the choice of the mathematical apparatus with which the mathematical model is built. Often differential equations, random processes, functions of complex form, time series with complex forms of behavior are used, the dynamic properties of which are practically impossible to study in detail by means of appropriate mathematical methods. The dynamic properties of cyclic trajectories can be thoroughly investigated only by transforming mathematical models into a recursive form. The theory of recursive functions allows to always perform the transition to the representation of models in recursive form[8]. The theory of recursive processes includes methods of iteration analysis in the study of the behavior of dynamic systems in any domain of its definition.

Iterations of mappings on an interval are undoubtedly the simplest models or examples of nonlinear (dissipative) dynamical systems. The mathematical theory of iterative mappings in general refers to the theory of recursive functions, the theory of dynamical systems, the theory of differential equations and is deeply connected with the modern chaos theory[11]. Dynamical systems use iterations of the form $x_n \to x_{n+1} = f(x_n)$, where the function is defined on the interval [0;1] and translates into itself and belongs to the class of primitive recursive functions[10]. Such iterative systems are the basis of methods of mathematical modeling of nonlinear processes in biology, chemistry, physics, economics, modern financial mathematics and other subject areas [12]. In general, one-dimensional mappings are similar to each other in one form or another. Abstracting from a detailed consideration, one can find many common results for, at first glance, quite different mappings.

A significant number of dynamical systems are modeled in continuous time by means of a differential expression of the form:

$$\frac{d}{dt} x(t) = f(x(t)) \tag{1.1}$$

where and – are a function on the phase space $\mathbb{R}^n$. An important example of such systems are the processes of population development in an environment with certain properties. The mathematical model of a stochastic dynamic system of population development can be represented in the following Fisher-Wright form [13]:

$$d x_\xi(t) = c \bullet \sum_{\xi' \in S} q_{\xi,\xi}\left(x_\xi(t) - x_\xi(t)\right) dt + \text{¿}$$

$$+ s \bullet x_\xi(t)\left(1 - x_\xi(t)\right) dt + \text{¿}$$

$$+ \sqrt{\gamma x_\xi(t)\left(1 - x_\xi(t)\right)}\, d\omega_\xi(t)$$

$$x_\xi(0) \in [0,1]\ \forall \xi \in S$$

This equation is reduced to an iterative form which will have the following form.

$$x_\xi(n+1) = x_\xi(n) + c \bullet \sum_{\xi' \in S} q(i,j)(x\text{¿¿}\xi'(n) - x_\xi(n)) + \text{¿¿}$$

$$+ s \bullet x_\xi(n)\left(1 - x_\xi(n)\right) + \gamma \sqrt{x_\xi(n)\left(1 - x_\xi(n)\right)}\, \omega(n)$$

The resulting iterative equation has a rather complex form. The behavior of such a dynamic system largely depends on the values of constants properties of the environment characteristics of changes in the genetic code of the population and the value of its drift [14]. As a process in the Fisher-Wright model, Wiener processes are considered, such as Brownian motion or geometric Brownian motion, which is everywhere positive and has a log-normal distribution law. It is proved that in the most general form such a dynamical system is described by a random process which is a martingale. Fundamental study of cyclic fixed points and their trajectories of such dynamical systems requires detailed information about the same characteristics of their components. The logistic component can be replaced by any other congruent, i.e. topologically equivalent nonlinear function. The class of such simple functions includes sin(nx) and (sin(nx))*1/2, and the square root of the logistic mapping due to the fact that they approximate the logistic mapping well, but the values of such functions are irrational numbers in the processes of recursive iterations. Such a set of intermediate values of recursive calculations in the processes of computer modeling leads to automatic rounding of intermediate values, which causes the appearance of chaotic components of a different nature, which necessitates a more correct analysis of the processes of their occurrence.

The Fisher-Wright model can be relatively easily adapted to model dynamic processes in stock markets, modern medicine, and this is especially true for the analysis of the dynamics of COVID-19 development, the analysis of the development of cloud technologies in semantic database theory and machine learning theory[].

It should be noted that dynamical systems defined by different mathematical mappings sometimes allow to obtain the same information. Thus, the study of trajectories of cyclic fixed points of mappings in the field of their definition, the analysis of the structure of trajectories of cyclic fixed points in order to find self-similar fragments of a certain degree in them and to find the laws of their distribution belongs to the set of actual mathematical problems. Another class of problems is related to the development of methods for estimating the fractal measure of sets, functions, random processes and the formation of information in systems and methods of controlling dynamic systems based on information about the structure of their cyclic trajectories.

Methods of structural analysis of cyclic trajectories of nonlinear dynamic systems

The results of the study of dynamic systems depend on the properties of quantities that characterize their representation in the form of their parameters. Systems may depend on many parameters, but the results of analysis and study of dynamical systems based on one-dimensional mappings can be applied to a wide range of complex dynamical systems.

Consider the mapping of the following classes: "Tent map", "Asymmetric tent map", <<D*iscontinuous tent* map>>, <<Saw>>, <<Logistic mapping>>, <<Root of logistic mapping>>, <<Sine>>, <<Algebraic mapping>> . This choice of mappings is due to the fact that some classes of complex mappings can be considered as functions of certain combinations of reduced mappings. In addition, between the reduced mappings there are dependencies that are a source of important information about the dependencies between classes of prime numbers used in the theory of discrete logarithm, in methods of constructing efficient pseudorandom number generators, and in the theory of numbers itself [6,7]. We will consider the given mappings in the form of the function f(x): R-R.

Then denotes the n-th iteration of the function $f(x)$. That is, is the n-fold composition of function with itself. If $x_0 \in \mathbb{R}$, , then the orbit or trajectory for is the sequence . Here are the definitions of the listed mappings.

When considering dynamic systems, fixed points, cyclic fixed points and their trajectories play an important role. The initial point is fixed under the condition $f(x_0)=x_0$. Based on this, we can conclude that the orbit of a fixed point is a constant sequence $x_0, x_0, x_{0,\ldots}$. These are such x_0, that $f^n(x_0)=x_0, n>0$, respectively, like closed orbits, periodic orbits repeat: . Further, periodic orbits of period will be called trajectories. For discrete dynamic systems we can distinguish several types of fixed points. Suppose that is a fixed point for f, then is called an attractor or attractive fixed point for f, if there exists a neighborhood of on the set with the property that, if the following conditions hold:

$y_0 \in U$, then for all and, moreover, $f^n(y_0) \rightarrow x_0, n \rightarrow \infty$. Similarly to this definition, is called a *repeller* or repulsive fixed point if all orbits (except x_0) leave during iterations of $f(x)$.

Let us consider the symmetric tent mapping and the algebraic mapping of the calculations of remainders modulo a prime number and with a base *a* greater than one and their behavior on the set of numbers 1/p provided that *p* is a prime number. In [8] it is proved that the number *a* under this condition is the classifier of the set of all primes. If we assume that card(g1)(1/p) is the length of the cyclic trajectory for a prime number p for the mapping g1(x), the following statement is true:

Statement 1. For any prime p, always p-1 is divisible by card(g1)(p) and its value (p-1)/card(g1)(p) always coincides with inda(p) for the algebraic mapping.

The validity of this statement is proved by computer simulation, the general principle of construction of which will be considered further. It follows that the symmetric tent mapping can be used to analyze the properties of prime numbers. At the same time, according to the results of the same computer simulation, it was found that the trajectories of the algebraic mapping and the symmetric awning mapping do not coincide in their structure, provided that they are reduced to the same scale of values along the ordinate axis. An important fact is that at large values of p cyclic trajectories of symmetric tent mapping are more suitable for the construction of efficient pseudorandom number generators than algebraic mapping trajectories. Despite the fact that the sawtooth mapping is considered to be one of the simplest examples of a nonlinear dynamical system, it demonstrates an important property that is characteristic of more complex algebraic mappings base a=2 on the set of primes. Similar to ***statement 1***, if card(g2)(p) is the length of the trajectory to map g2(x) for x0=1/p then the following statement is true:

Statement 2. For any prime number p>3, always p-1 is divisible by card(g2)(p) and its value (p-1)/card(g2)(p) coincides with ind2(p) for the algebraic mapping provided that a=2.

The validity of this statement immediately follows from the fact that in the mapping g2(x) at each iteration the value of the numerator of the fraction coincides with the value of the corresponding iteration of the algebraic mapping. Thus, the mapping g2(x) can be used to analyze the classification of prime numbers, construct pseudo-prime number generators and model complex dynamical systems as a component of the model [9].

Consider the reflection g3(x) has a break point, i.e. it can be considered as a reflection of the tent with a break at x=1/2. At the break point g3(1/2)=1/2 in this model, but the break can take other values. In the series of papers [13,14] it was proved that on the set of numbers x0=1/p this mapping has cyclic trajectories whose length card(g3(x))(1/p) in general does not divide (p-1) despite the fact that the mapping can be classified as a d*iscontinuous tent* map. The dynamic properties of this mapping indicate that the lack of information about the properties of cyclic trajectories can lead to its incorrect use in the approximation of complex dynamical systems by such components. This fact indicates that when modeling dynamic systems it is necessary to have accurate information about the properties of the components of mathematical models. This fact is important even when analyzing fixed points of absolute shape. This is evidenced by the behavior of the awning reflection at the point x = 0.666. In general, the mapping may have a significant number of such fixed points and if their location is not taken into account, the lack of information about such points can lead to gross errors in the modeling process. These facts indicate that when modeling such dynamic systems of population development it is necessary to have sufficiently accurate information about the properties of all components of the mathematical model.

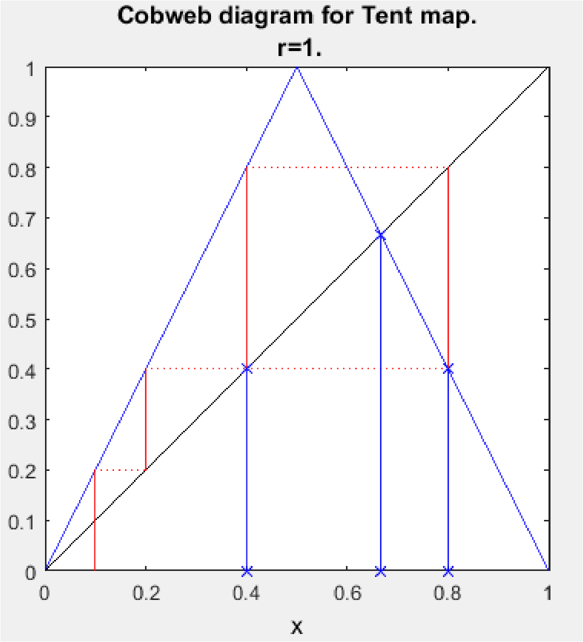


Figure 1 Cobweb diagram of the symmetric tent, n = 50

Note that the point does not move at all, that is $f^n(\bar{x})=f(\bar{x})=\bar{x}$. is a *fixed point* of the mapping f. Practically, this means that if the system hits the point at any moment, she will stay there forever. Figure 1 also shows an equally important property - *periodic orbit.* First of all, let's notice 2 new fixed points: and $\bar{x}_2=0{,}8$. It is easy to see that and $f(\bar{x}_2)=\bar{x}_1$, or, in other words, та $f^2(\bar{x}_2)=\bar{x}_2$. This observation suggests that the given mapping has a periodic orbit of length 2 (based on the fact that has 2 fixed points $\bar{x}_1, \bar{x}_2$, that are not fixed points of f).

From this knowledge follows a crucial question: if a fixed point, or periodic point, exists in the considered dynamical system, does it arise at small system perturbations? In the context of nonlinear dynamical systems, we can distinguish the following types of disturbances:

- disturbance of the initial state: "Is the behavior and development of systems that have similar initial states similar?";

- disturbance of the function f: "f is only approximately defined";
- stochastic disturbances: "In fact, the expression looks different, but micro-noises can be taken into account by an additional coefficient $x_n = f(x_{n-1}) + r(x_{n-1})$, where is a small random step, i.e. a small variation with some existing distribution possibility".

The study of the behavior of cyclic trajectories of fixed points of reflection not symmetric tent is no less important task of creating a fundamental theory of complex dynamical systems. In the series of works [15], a deep, and one can say, a complete study of attractors of this class of reflections was performed. However, there is no information about the structure of their trajectories. It is necessary to create methods that would allow under any circumstances to have detailed information about their properties. The basics of such a method were proposed in [16].

Also, the subject of research of dynamical systems is the asymmetric "tent" mapping . It can be considered as an extension of the standard "tent":

$$f(x) = x_{n+1} = \begin{cases} \dfrac{x_n}{a}, 0 \le x_n \le a \\ \dfrac{1 - x_n}{1 - a}, a \le x_n \le 1 \end{cases} \qquad (1.4)$$

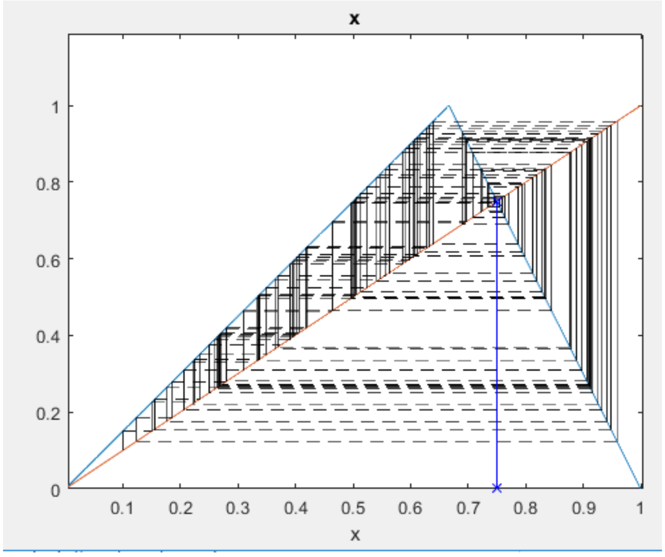


Figure 2 Cobweb diagram of the asymmetric tent, n = 100

By analogy with the symmetric tent, a cobweb diagram is constructed (Figure 2). You can immediately see that after 100 iterations, the asymmetric tent shows a chaotic structure: iterations are constantly approaching a fixed point $\bar{x}=0{,}7502$, but no stabilization of the structure occurs. In addition, the chaotic behavior of is shown in Figure 3. The essence of chaos is that the values of periodically approach each other, but never self-replicate.

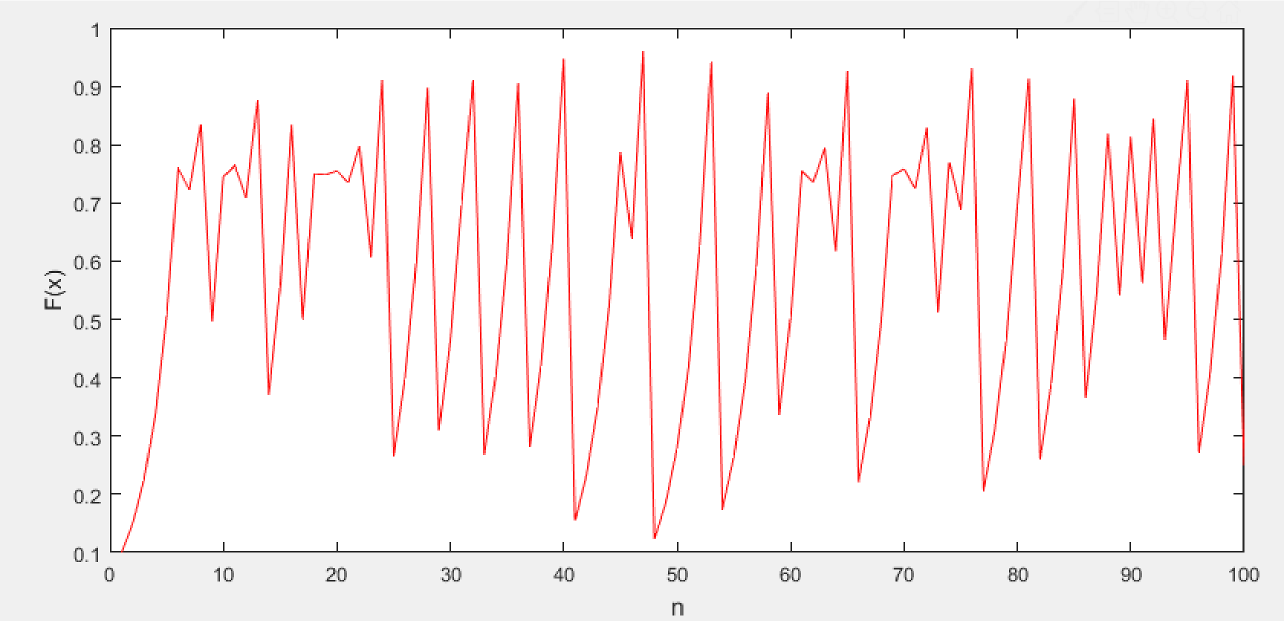


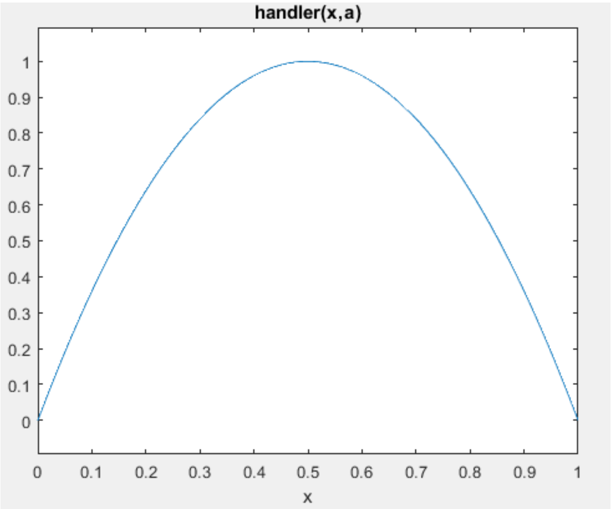
Figure 3 «Chaotic» structure of the asymmetric tent

1.1 Logistic mapping

Logistic mapping is usually specified as follows:

$$f(x) = x_{n+1} = r x_n (1 - x_n) \tag{1.5}$$

where is the operator that fixes the population growth. Logistic mapping also demonstrates the basic properties of nonlinear dynamical systems. In this paper we will use the logistic mapping for when there are signs of chaotic behavior. An example of the



mapping is shown in Figure 4.

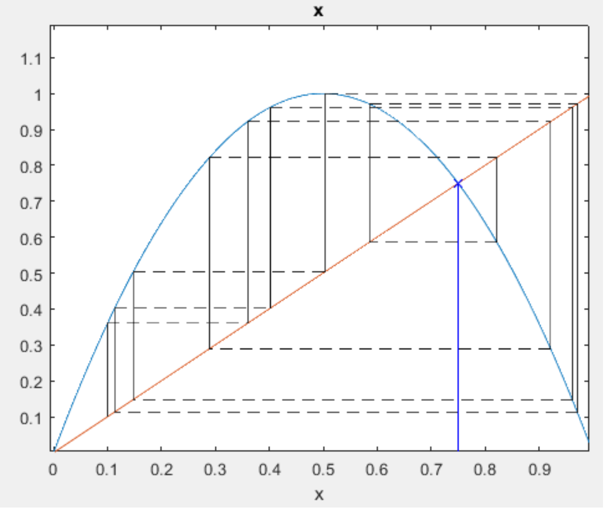


Figure 4. Logistic map $x_0=0.1$, $\bar{x}=0.7509$

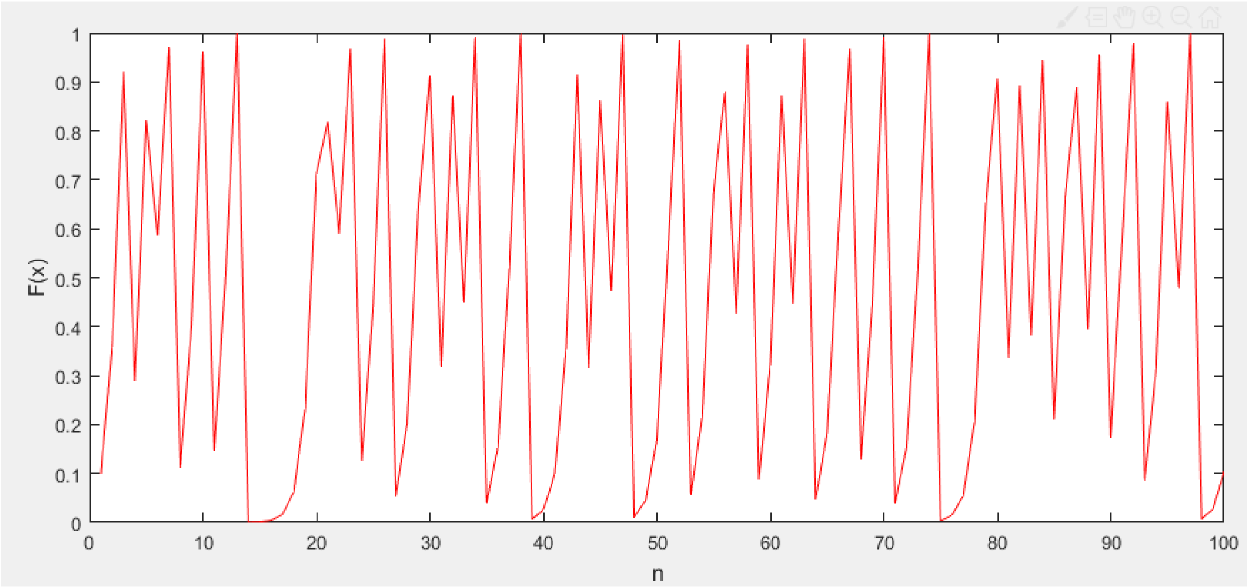


Figure 5 «Chaotic» structure of the logistic map

1.2 Sine mapping

The provided mapping is very similar in structure to the logistic one. An example of its construction is shown in Figure 6.

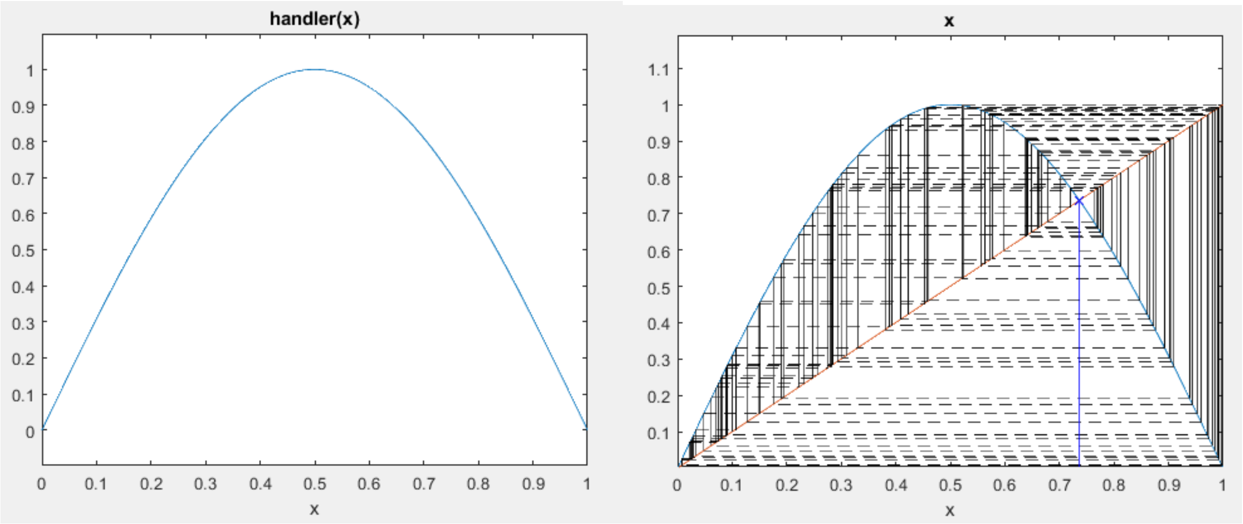


Figure 6. Map $f(x) = \sin(\pi x)$*, ,* $\overline{x}=0.7367$

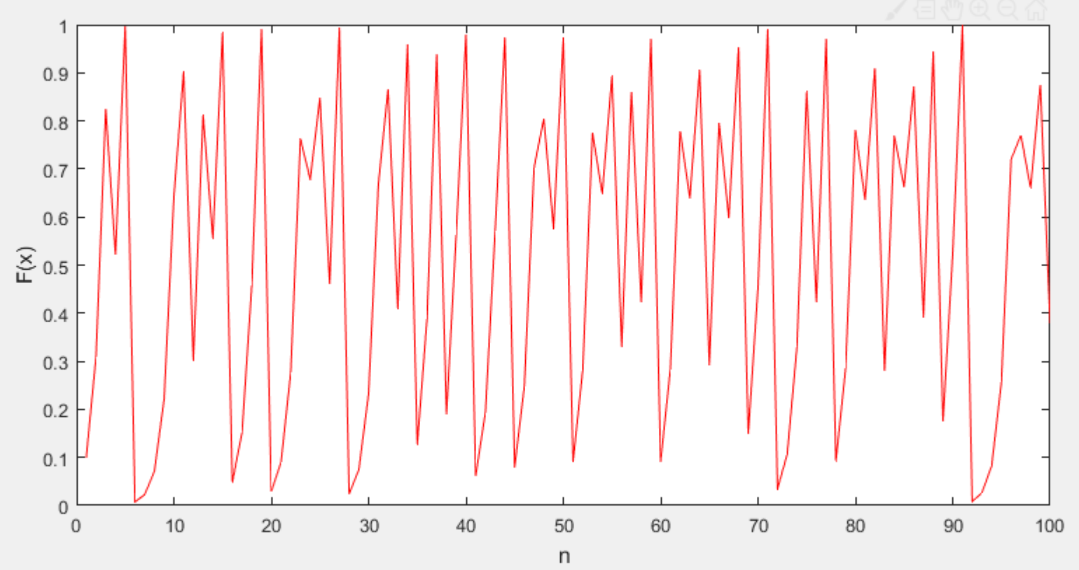


Figure 7 «Chaotic» structure of $f(x)=\sin \pi x$

1.3 The degree of similarity of the considered reflections

In some sense, the considered one-dimensional mappings demonstrate similar behavior of the corresponding nonlinear dynamical systems. All of them demonstrate the so-called chaotic behavior, because they are sensitive to initial conditions. Usually, the given mappings are considered on the interval [0,1], taking into account the significant similarity of their structures, which is clearly shown in Figure 8.

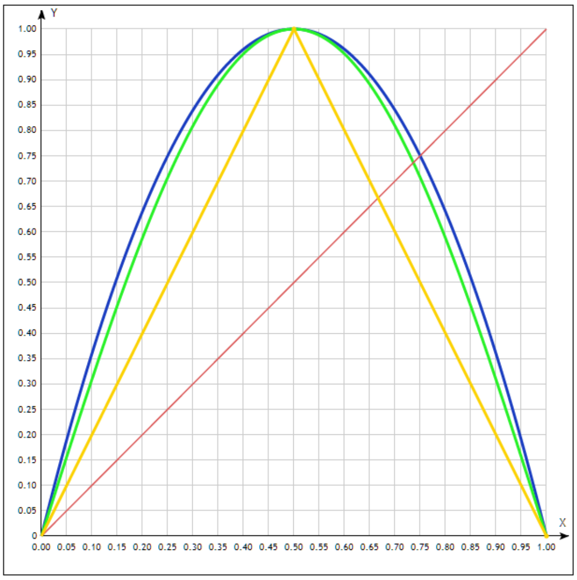


Figure 8. Mappings: tent, logistic,

SECTION 2

2.1 Topological conjugacy of one-dimensional mappings

Consider the tent mapping:

$$f_1(x) = x_{n+1} = \begin{cases} 2x_n, x_n < \dfrac{1}{2} \\ 1- 2x_n, x_n \geq \dfrac{1}{2} \end{cases}$$

The graph for contains tents with width 2^{1-n}. The distance between adjacent n-cycles is at most 2^{2-n}. For any compact subinterval $]0,1[$ there exists a constant independent of n, such that the distance between adjacent n-cycles satisfies the condition $c^{2-n} < distance < 2^{-n}$. The mapping (2.1) is notable for the fact that it shares many properties with the logistic mapping in the iteration process. This feature indicates their conjugacy. If we assume that I and J represent some intervals for the mappings $f: I \rightarrow I, g: J \rightarrow J$. Then we can say that the mappings and are conjugate if there exists a homeomorphism $h: I \rightarrow J$, such that satisfies the conjugacy equality $h \circ f = g \circ h$. Conjugacy maps orbits to orbits g. This follows from the fact that for all such that maps the n-th orbit point for from to the n-th orbit point of $h(x)$.

Theorem 3: The tent mapping is congruent with the logistic mapping, the root of the logistic mapping and the sin(nx) mapping.

The proof is based on the following sequence of steps that follow from the paper[16].

Step 1. *If there is a topological conjugacy, then the values at the ends of all n-cycles are uniquely determined.*

A congruence or homeomorphism of H must map a nonzero cyclic fixed point from to a nonzero cyclic fixed point from g.

Fixed points must be mapped to a corresponding number of fixed points in ascending order. The corresponding mapping on the fixed points has already been determined. Given this fact, it is not obvious that the fixed points can be mapped in increasing order. For example, if there are two fixed points in between all fixed points of and only one fixed point between all fixed points of g.

Necessary and sufficient condition for the correct ordering of quantities is the following: for each and $1 \leq m \leq 2^n$, defined by $x_{m,n}$, m-th n-cycle f^n, counting from the left, and analogues of cycles for g^n, is true for each and if and only if $y_{j,k} \epsilon$¿$y_{m,n}, y_{m+1,n}$¿.

We prove that this statement satisfies the existence of the j-th fixed point f^k. We call one of the intervals of length $2^{-k}2$ as J. All intervals of size are to the left of the interval containing the fixed points f^n, lying to the left. To determine the order, we only need to consider the interval of width 2^{-n}, starting from the left edge J.

Intervals of length are assumed to be non-strict on the left and strict on the right. Then the fixed points lie exactly on one of the intervals of length connected in y J. We call this small interval K. Compared to the two fixed points in K, the j-th point can be either to the left or to the right of the center.

It follows that the values of all$n$-cycles is uniquely determined. This defines as a dense set.

Step 2. *It is enough to show that the mapping defined on the cycles extends to a continuous function on the interval [0,1].*

From the constraint on h, which requires the set of cycles to be strictly ordered, it follows that any continuous expansion will be non-decreasing. In order to show that it is in fact strictly increasing, suppose that $x_1 < x_2$. Choose two cycles between and x_2. Then $h(x_1) \le h(\tilde{x}_1) \le h(\tilde{x}_2) \le h(x_2)$, which shows that is strictly monotonic.

Step 3. *Building a continuous expansion.*

To extend the interval to the open subinterval]0,1[it is enough to extend every compact subinterval [a,b]]0,1[. To extend [a,b], it is enough (and necessary) to show that if are sequences of the cycles in [a,b] where $z_n - w_n \to 0$, then $h(z_n) - h(w_n) \to 0$.

To prove the sufficient condition, we denote and as the degrees of and w_n. Renaming and w_n, we assume that $r(n) > s(n)$. Since $0 \neq z_n - w_n \to 0$, it follows that $r(n) \to \infty$. In addition, the nearest cycle to w_n, and hence to z_n, is almost at a distance from z_a, hence it follows that $z_n - \tilde{z}_n \to 0$. Suppose that the degrees and between fixed points are separated by $j_n > 0$.In this case, if and only if $j_n / 2^n \to 0$.

The mappings and are fixed points of and is the j_n-th neighbor of among similar cycles. This follows from $\left|h(z_n) - h(\tilde{z}_n)\right| \le C j_n 2^{-n} \to 0$. Since is between and $\tilde{z}_n$, it follows that $\left|h(z_n) - h(w_n)\right| \le \left|h(z_n) - h(\tilde{z}_n)\right| \to 0$. This confirms the sufficient condition for continuous expansion. It follows that is expanded on the continuous function on the interval]0,1[.

To complete the proof it suffices to show that and $\lim_{x \to 1} h(1) = 1$. The largest of the n-cycles, x_n, the tent mapping and its mapping converge to 1. Since is monotonic on [0,1], it follows that $x \to 1$, $h(x) \to 1$. Considering the smallest n-cycle in]0,1[proves that $\lim_{x \to 0} h(x) = 0$. Moreover, becomes expanded: it is continuous on [0,1].

Thus, it was shown and proved that the tent mapping and the logistic mapping are congruent and equivalently topologically conjugate. Of course, this is also true for the asymmetric case of the tent and the root of the logistic mapping. The fact that the mapping of type is congruent to the logistic mapping follows from the following simple transformations. Let us define the conjugacy equation by analogy with the definition of the logistic mapping when a = 4:

$$h(2x)=4h(x)(1-h(x)), \tag{2.2}$$

for note that the above satisfies the function of the form

$$h(x)=\sin^2(cx), \tag{2.3}$$

for any by formula $\sin(2\theta)=2\sin\theta\cos\theta$.

In order for to be a homeomorphism of an interval onto itself, it must be monotone on any interval. If we look closely at the homeomorphism defined by formula (2.3), it makes sense to consider $c=\frac{\pi}{2}$. It follows that $h(0)=0$, and is increasing on the whole interval $[0,1]$.

To make sure that (2.3) is indeed a topological conjugation, it is necessary to check it on the interval $x\in\left[\frac{1}{2},1\right]$:

$$h(2(1-x))=4h(x)(1-h(x)) \tag{2.4}$$

Let's perform substitution and simplification:

$$h(2(1-x))=\sin^2(\pi(1-x))=\sin^2(\pi x)=¿$$

$$¿4\sin^2\left(\frac{\pi x}{2}\right)\cos^2\left(\frac{\pi x}{2}\right)=4h(x)(1-h(x)) \tag{2.5}$$

That was to be proved.

The proved statement allows us to consider the mapping of the form as an example of a topologically conjugate system with logistic mapping and tent mapping. From this theorem follows only the fact that in congruent cyclic fixed points the mappings have the same lengths of cyclic trajectories, but their structures can be different and to a large extent. The values of these mappings belong to different classes of numbers. The values of the cyclic trajectories of the tent and logistic mappings take rational values, and the root of the logistic mapping belongs to the class of algebraic numbers, and the function *sin(nx)* is the value of the real numbers, which in general are transcendental. These facts must be taken into account when modeling the behavior of such dynamic systems even on powerful modern computers due to the fact that automatic rounding of values can lead to an automatic transition to a completely different cyclic trajectory.

2.2 Analysis of structures of cyclic trajectories of fixed points of reflections.

To solve many applied problems, for example, the creation of pseudorandom sequence generators, the theory of redundancy modulo a huge ordinary number, with base a being the original root of the chosen p, is systematically used. In this case, based on the Fermat theory [], the equation $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ is the basis of the iterative procedure:

$$x_0 = 1, \quad x_{n+1} = ax_n (\mathrm{mod}\, p) \tag{2.6}$$

Using a certain iterative process, a sequence of values is obtained in the form of a set $\{x_0, x_1, \cdots, x_n, \cdots, x_{p-1} = 1\}$, which is interpreted as a pseudorandom sequence. Based on the statistical analysis, it is proved that for large values of p the sequences for all the primitive roots are given $\{a, \cdots, a_{\varphi(p-1)}\}$, where $\varphi(p-1)$ is the Euler function, all variant-rich sequences have a similar property, which can be interpreted as chaos.

The mapping $f(x)\equiv ax^n(\bmod p)$ is clearly related to the group of residues (Z/pZ)∗ modulo p. If a is a primitive root of a prime number p. then it is easy to prove that a is a generating element of this group, and the iterative process (2.6) determines a permutation on the set $\{1,2,3,4,\cdots,p-1\}$, that forms a cyclic permutation subgroup of order p of the complete permutation group on this set. This simple fact is an important basis to argue that such a group cannot have a chaotic structure. This statement can be demonstrated by the example when $p=19$, and all six primitive $\{2,3,10,13,14,15\}$. At the same time $\varphi(19-1)=\varphi(2\cdot 3^2)$. For this set of original roots, the following permutations are obtained based on the iterative procedure (1):

a	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*
2	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	1	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
10	1	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
13	1	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	1	14	6	8	11	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	1	15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1

Table 1

From the above example it follows that for $p=19$ there is a clear structure of permutations. It is proved that for any prime number p, of arbitrarily large value, the set of all its primitive roots has a structure defined by the decomposition into prime factors of the number $p-1=\prod_{i=1}^{k} p_i^{\alpha_i}$. In the above example $p=19$ and $p-1=2\cdot 3^2$. The effect of factors 2 and 3 can be seen from Table 1.

Thus, the given sequence has a clear structure, which does not allow us to consider it a chaotic system. Let us try to find similar structures in the group of pairwise congruent mappings (1.4), (1.5) and (1.6).

2.3 Analysis of structures of one-dimensional mappings

Despite the simplicity of the above mappings, their structure largely depends not only on the properties of the functions used in their construction, but also on the properties of the numbers used as initial conditions and parameters. These mappings allow us to divide the set of primes *p* into a system of classes based on the length of the iterative process for given primes []. Note that there are many prime numbers for which the length of the period is significantly less than the dimension of the number. The sequence obtained for this number forms a simple structure. Simple structures are characteristic of the Fermat, Mersenne, and their various generalizations. At the same time, other prime numbers generate sequences for which the length of the period is proportional to its dimension and, accordingly, can demonstrate a greater degree of approximation to randomness, but also have periodic elements, as demonstrated in Figures 11-13.

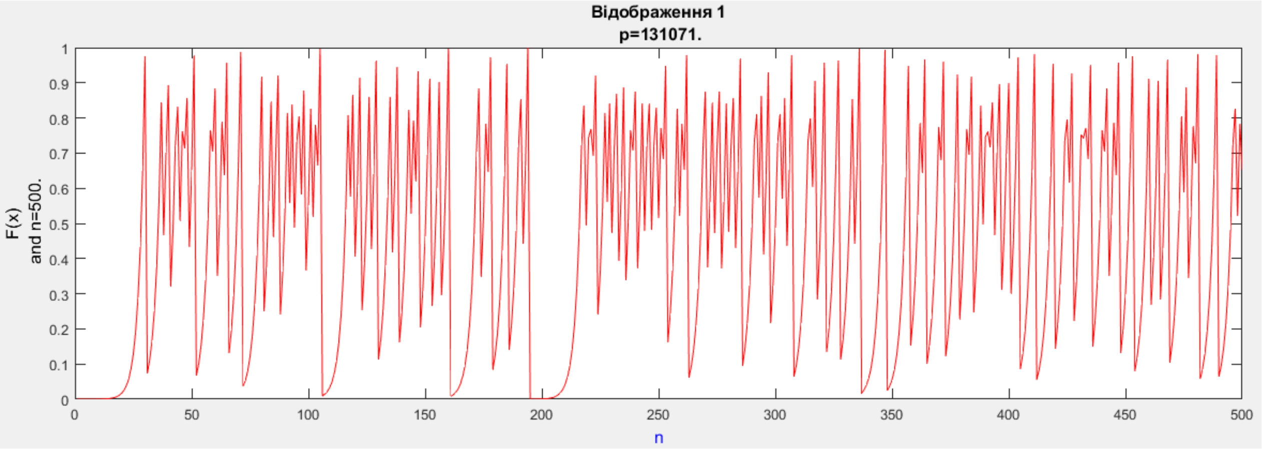


Figure 11. Mapping (1.4)

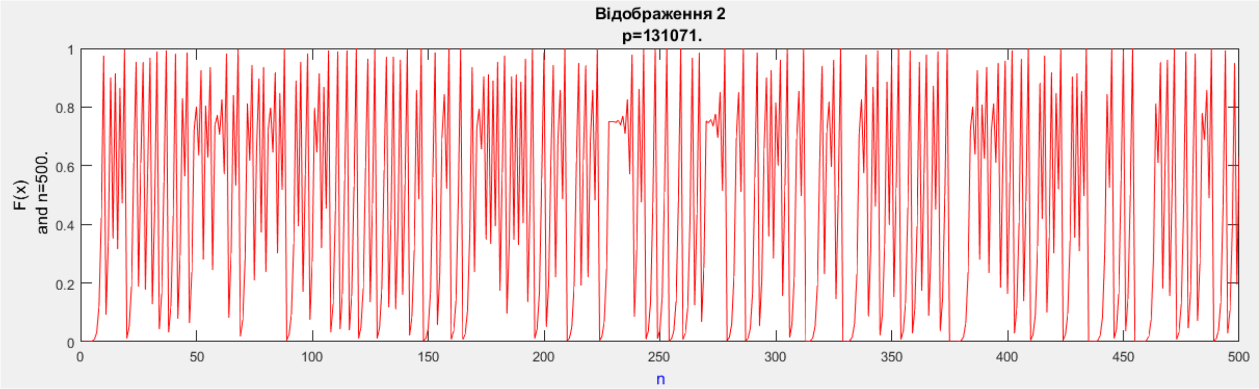


Figure 12. Mapping (1.5)

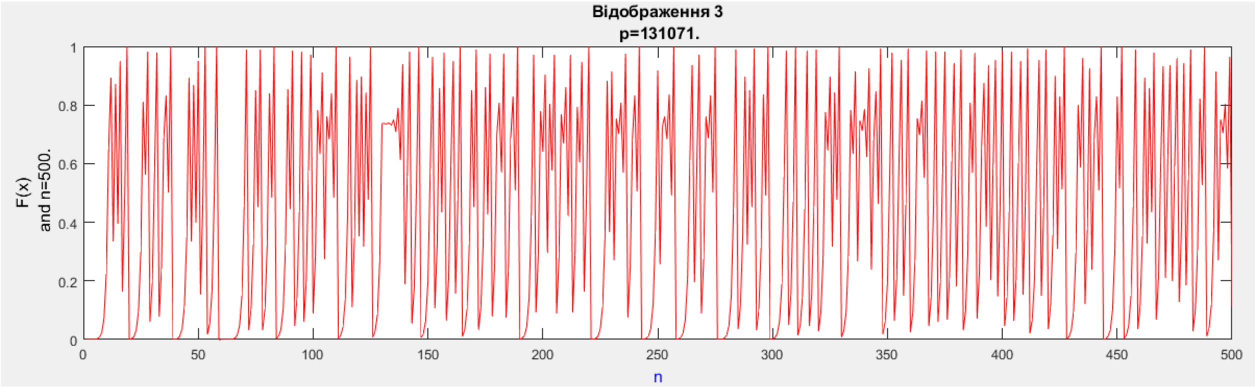


Figure 13. Mapping (1.6)

At first glance, the sequence generated by the mapping (1.5) has a higher density, i.e. it tends to have a uniform distribution law, but looking at the internal structure of the sequences, a certain degree of similarity should be introduced. For example, for a given prime p = 131071, Figures 14-16 show the structure of iterative processes for mappings, where the dashed line shows the resulting sequences, the solid line shows the internal elements of the sequences that give the highest value of the similarity measure.

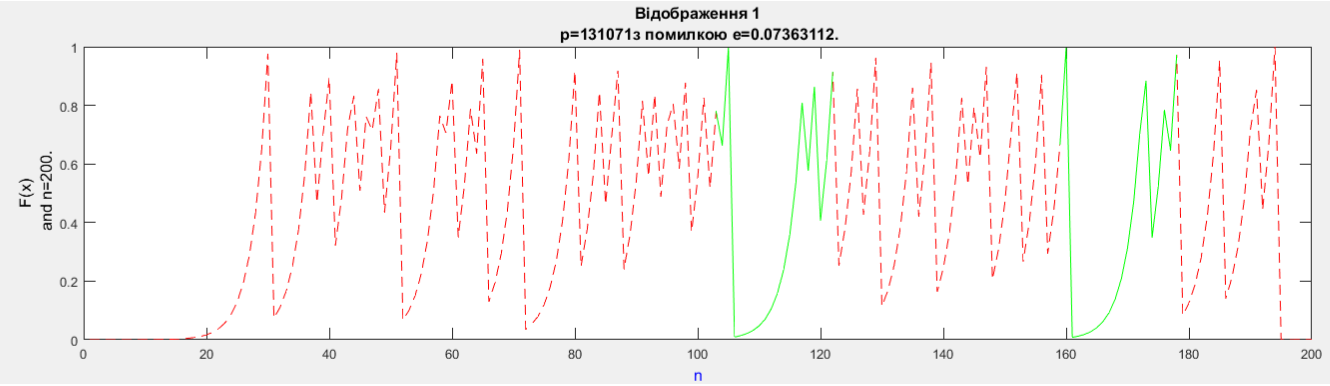


Figure 14. Internal structure of the mapping (1.4)

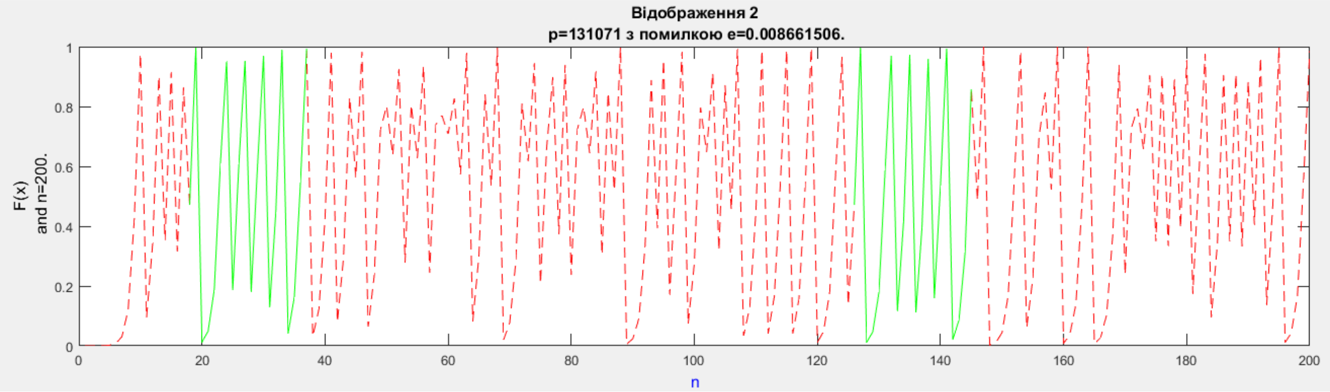


Figure 15. Internal structure of the mapping (1.5)

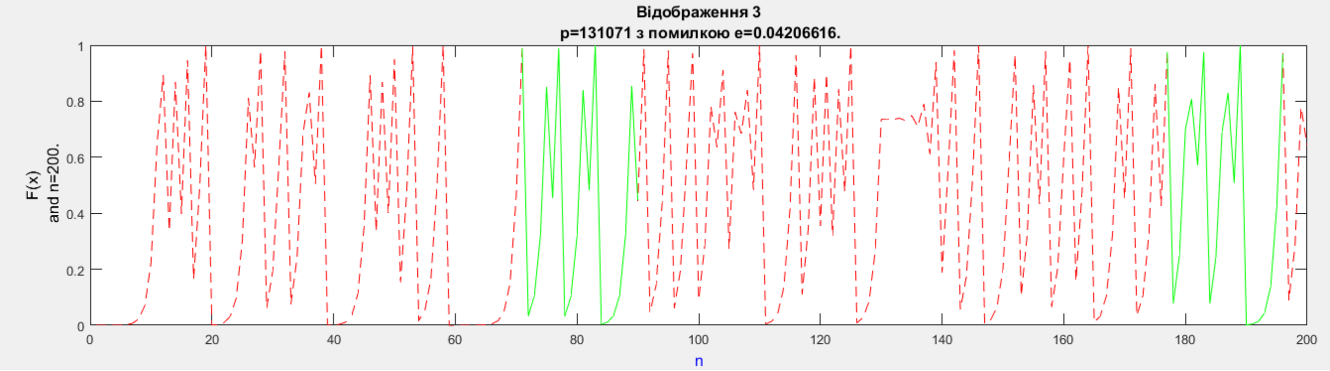


Figure 16. Internal structure of the mapping (1.6)

As can be seen in these figures, the sequences obtained using mappings (1.5) and (1.6) for some subsequences give similarity values close to 0, indicating the influence of fixed points on the internal structure of the sequence.

2.4 Methods for estimating the degree of randomness

There are several approaches to the definition of randomness and, accordingly, methods for assessing the degree of randomness of a certain sequence. In [7], four algorithmic properties are distinguished to describe randomness: frequency stability, chaoticity, typicality, unpredictability. Each of them represents its own algorithmic aspect of randomness, and each of them, with a greater or lesser degree, can claim to be a mathematical definition of randomness. In this case, sequences in binary format are considered. According to Mises' definition, sequences are divided into 2 groups: random and non-random. From a mathematical point of view, random sequences form a set of full measure and all without exception satisfy all the laws of probability theory. In this approach, a sequence is considered random if there is stability of frequencies 0 and 1 both in the sequence itself and in any "correctly" selected part of it. According to Mises, an acceptable selection rule is that the decision to include a member in the subsequence cannot depend on the value . It is worth noting that the class of "admissible" frequency stable sequences for which the basic laws of probability theory are fulfilled has not yet been defined. It was also proved the existence of sequences that satisfy the requirements of Mises, but do not satisfy the law of repeated logarithm.

The approach proposed by Martin-Löf is that a sequence is considered random if it passes a certain set of statistical tests. The essence of testing is to check the "null hypothesis" about the sequence under study. A statistical test T for binary sequences of length l can be viewed as a Boolean function that divides the set of sequences into a set of "non-random" sequences (usually small) and a set of random sequences. The probability *pr* that a randomly chosen sequence of length l is rejected by the test is $pr=|V_{l,0}|\cdot 2^{-l}$. As a rule, in tests is small, $pr\leq 0.01$. Since it is possible to prove analytically some of the necessary properties only for some classes of sequences, a wide range of different statistical tests are used to substantiate the properties of sequences, which allow to identify patterns. The results of the statistical tests show that for mappings 1.5 and 1.6, the sequences exhibit the best measure of randomness on individual tests, however, this is not true for the entire group of tests.

This paper also analyzes the chaotic nature and unpredictability of the internal structure of generated sequences to form the concept of a truly random sequence. When considering the concept of randomness, the Kolmogorov complexity theory is used, where the main idea is based on the fact that the complexity of an object is determined by the length of its description. The complexity of a sequence for a given mapping *f* is a number where |x| is the length of the sequence. If an object cannot be described, respectively, its complexity approaches infinity. When the internal structure of numerical sequences is considered, the presence of internal similar subsequences means that these internal structures can be grouped into separate classes and a description can be assigned to each class, which reduces the size of the description of the entire sequence. Thus, when considering the internal structure of the formed sequences, the closest to chaotic sequences will be those that have the least degree of similarity.

Moving on to unpredictability, we understand a sequence as unpredictable if, given an arbitrary choice of its elements, knowledge about these elements does not allow predicting the value of the next elements of the sequence. Since this paper studies processes in nonlinear dynamical systems, unpredictability is the result of sensitivity to the initial conditions of the systems. A sequence is called predictable if there exists a mapping for it that allows to obtain a sequence element based on previous values. Thus, periodic similar subsequences allow to calculate sequence elements with a certain level of similarity. It is known that any chaotic sequence is unpredictable. However, the question of coincidence of classes of chaotic and unpredictable sequences remains open.

Given the internal structure of the sequences obtained on the basis of the above mappings, the problem of finding and evaluating such structures arises. The presence or absence of which reflects a certain degree of approximation of this sequence to randomness. Hence, the problem of choosing a similarity measure to evaluate the obtained sequences arises. In general, the similarity measure allows to generalize the structural representation of the object.

Let us consider the existing approaches and methods for estimating the similarity measure. The first type of similarity measure evaluates and compares the overall shape of subsequences based on the actual values of the sequence. Two subcategories can be distinguished: rigid stepwise and elastic measures. Rigid stepwise measures require both sequences to be of the same length, whereas elastic measures are more flexible and allow "one-to-many" and "one-to-one" comparisons for subsequence elements [8]. The second type of similarity measure, characteristic measures, where first the properties of a subsequence are determined and then the distance between these characteristics is measured. Characteristic measures are often used to reduce the dimensionality of the evaluated objects. The third category, edit distance, expresses the mismatch between two subsequences based on the minimum number of operations required to transform one subsequence into another.

The simplest similarity measure for comparing subsequences is any norm of the kind:

$$d_{L_n}(x,y)=\left(\sum_{i=1}^{M}(x_i-y_i)^n\right)^{\frac{1}{n}} \tag{2.1}$$

where n is an integer, M is the length of the subsequence. Norm-based measures belong to the category of hard stepwise measures and compare structures of the same length. In the case when n = 2, we obtain the Euclidean norm, the evaluation process of which is shown in Figure 17.

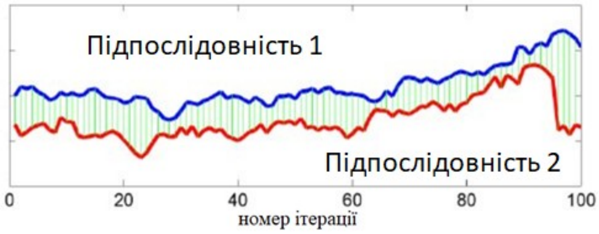


Figure 17. Sequence comparison process

However, such measures do not identify the similarity of subsequences if they are not aligned according to all X. Accordingly, the problem of "deformation" of the values of all X for one of the subsequences arises. This problem can be solved by elastic measures, such as the method of dynamic scale transformation (DST) [12], but such measures increase the complexity of calculations and the time required to obtain the result. When determining the DST measure, the local cost matrix (LC) is first calculated (n × m), where each element of the matrix determines the distance between the corresponding elements of the subsequences. The next step is to determine the transformation path:

$$W = w_1, w_{2,\dots} w_k, min(n, m) \le k \le m + n + 1 \qquad (2.2)$$

This path traverses the LC matrix with such conditions as: boundary condition, continuity, monotonicity. The total distance for the path W is determined by summing the individual elements of the matrix LC that the path covers. To obtain the DST measure, it is necessary to choose the path with the minimum total distance. The computational complexity in this case is *O(nm)* when using dynamic programming (DP) methods. The following DP recurrence relation can be used to calculate the path with minimum length:

$$d_{cum}(i, j) = d(x_i, y_i) + \{d_{cum}(i-1, j-1), d_{cum}(i-1, j), d_{cum}(i, j-1)\} \quad (2.3)$$

To obtain the DST measure directly, several scales have been developed, one of which is the root of the sum of path elements with minimum length:

$$d_{DTW}(x, y) = \sqrt{\sum_{k=1}^{K} w_k} \qquad (2.4)$$

It is worth noting that the DST measure is equal to the Euclidean norm if $n = m$. Due to the need to calculate matrices, this method is one of the most time-consuming, even under optimization conditions, so it is not considered in this paper.

The next group of similarity measures is represented by characteristic measures, among which the main one is the Discrete Fourier Transformation (DFT). As noted above, this measure evaluates the characteristics of the compared structures and, since it is calculated only for half of the elements of the subsequence according to the Nyquist-Shannon counting theorem, allows to obtain a gain in the total computation time. DST is obtained by computing the product between a subsequence and a sinusoid and is defined as:

$$X(1)=\sum_{k=0}^{N-1} x_k e^{-i\frac{2\pi lk}{n}} \tag{2.5}$$

As a result, we get a vector of complex numbers. According to the Parseval theorem, the DFT preserves the Euclidean distance between sequences. That is, when all frequencies from the frequency domain are used, the Euclidean distance between two DFTs is equal to the distance between the original sequences for these transformations, since the DFT is a linear transformation. The calculation of the distance between sequences based on Fourier coefficients is *O(q)* and therefore the whole process of calculating the DFT measure for all subsequences is $O(Nn\log n+qN^2)$, where N is the number of all subsequences.

2.5 Computer tools to perform this research

Computer representation of the structure and behavior of dynamic systems is at the heart of the development of modern complex systems. Such representations are created and revised based on the use of graphical modeling languages that support the specification, analysis, development and verification of systems.

To perform the tasks and software implementation, the Matlab language and the MATLAB R2018b development environment were chosen []. Matlab programming language supports development based on various programming paradigms with an emphasis on functional programming. It has a large set of built-in functions, graphing tools, and also allows you to implement dynamic interactive calculations that allow you to manipulate data and analyze the dynamically changing result. Matlab system provides a wide set of higher-order functions, meta-algorithms with the help of which an advanced multi-level environment with automation is implemented when building user interfaces. Built-in sets of functions allow you to implement algorithms of various mathematical areas, such as number theory, dynamical systems and others. Matlab system also implements the possibilities of parallel programming, which allows to reduce computation time. The system supports numbers of any precision, and to increase the accuracy, the environment uses symbolic calculations that allow you to transform expressions. A large number of statistical distributions and a set of statistical functions and operations allows you to evaluate and test hypotheses, analyze models, etc.

Matlab has a large number of functions for building graphs, including three-dimensional, visual data analysis and creating animated videos.

The built-in development environment allows you to create graphical interfaces with various controls, such as buttons, input fields and others.

Key features:

- platform-independent high-level programming language focused on matrix operations and algorithm development;
- interactive environment for code development, file and data management;
- functions of linear and nonlinear algebra, statistics, Fourier analysis, solution of differential equations, etc;
- extensive graphics visualization tools;
- built-in user interface development tools for creating standalone programs;

- C/C++ integration tools, code inheritance, ActiveX technology.

2.6 Computer modeling of dynamic systems

B In this paper, we consider the application of the shape estimation measure and the DFT measure as an example of a characteristic measure, since they provide a simple computational process and allow us to draw conclusions about the internal structure of the sequences considered in this paper. The correlation coefficient based measure is chosen as a hard stepwise measure. Among the various correlation coefficients we will use Spearman correlation because Spearman correlation coefficient does not make any assumptions about the distribution of the data and is an appropriate correlation analysis when the variables are measured on a scale that is at least ordinal. Sequences will be called similar if the measure takes a value greater than 0.5. Spearman correlation does not imply a linear type of relationship between the compared values. It also helps to reduce the effect of extreme fluctuations in the values of the subsequent sequence. The Spearman correlation coefficient can be calculated using the following equation:

$$r_s = 1 - \frac{6\Sigma d_i^2}{N\left(N^2 - 1\right)}, \tag{2.6}$$

where is the difference between the rank for each data pair and N is the number of data pairs. Spearman correlation performs analysis based on the rank of the data, so it can represent the similarity of the shape of two distributions. Spearman's correlation coefficient calculates p-values in the same way as linear regression and Pearson's correlation, except that the calculation is for ranks rather than magnitude. It should be noted that the price for the better properties of the Spearman correlation is the higher computational complexity which is *O(n log n)*, while the Pearson correlation has a complexity of *O(n)*. However, modern parallel computing methods allow to minimize this time difference. To estimate the internal structure of the sequences obtained from the mappings, a method is used that includes the following steps:

Step 1. The position of the first peak is calculated in order to remove the initial exponential component from consideration;

Step 2. The size of the initial subsequence to be estimated with the subsequent sequence elements is determined;

Step 3. Using a unit step, the Spearman correlation value of the reference subsequence with the corresponding size subsequences is calculated;

Step 4. The obtained correlation values are filtered according to the specified similarity level;

Step 5. The size of the initial subsequence is reduced by 1 if it exceeds 10 elements, and steps 1-4 are repeated.

Thus, this method allows to obtain a hierarchy of internal cycles according to the length of the cycle as well as the degree of similarity of the found structures. This hierarchy can be used for further sequence evaluation. According to the step-by-step approach to finding similar subsequences, we obtain a set of values that could identify a subsequence that exceeds the initial score.

Considering the results for individual sequences, the results of similarity measure estimation allow to obtain a hierarchy of similar subsequences based on the length of internal loops and their similarity level, which is presented in Table 2.

s	l	pat	comp	lag	SM
11	**0,6**	{9, 19}	{20, 30}	4	**0,636364**
11	**0,7**	{9, 19}	{20, 30}	36	**0,772727**
11	**0,8**	{17, 27}	{28, 38}	33	**0,836364**
11	**0,9**	{40, 50}	{51, 61}	53	**0,972727**
15	**0,6**	{11, 25}	{26, 40}	29	**0,614286**
15	**0,7**	{19, 33}	{34, 48}	67	**0,717857**
15	**0,8**	{36, 50}	{51, 65}	49	**0,817857**
15	**0,9**	{13, 27}	{28, 42}	67	**0,907143**
20	**0,6**	{12, 31}	{32, 51}	12	**0,637594**
20	**0,7**	{11, 30}	{31, 50}	62	**0,795489**
20	**0,8**	{13, 32}	{33, 52}	62	**0,842105**
25	**0,6**	{10, 34}	{35, 59}	57	**0,66**
25	**0,6**	{30, 54}	{55, 79}	13	0,616923
25	**0,7**	{50, 74}	{75, 99}	6	0,731538
30	**0,6**	{10, 39}	{40, 69}	52	0,631146

Table 2 Similar subsequences for mapping 1.4 and p=521

Comparing the selected similarity measures, the DFT measure demonstrates the best results in finding similar subsequences, since it represents the evaluation of the subsequence as a sum of harmonic oscillations, respectively, allows a more accurate evaluation. Also, the DFT measure has better computational performance due to the reduction of dimensionality, which significantly affects the overall computation time for sequences that exhibit a period length commensurate with a prime number.

The time complexity for the DFT when using the fast Fourier transform algorithm is *O(n log n).*

The results show that from the point of view of chaotic and unpredictability, the considered mappings 1.4 and 1.5 show a very high degree of similarity for many internal cycles. The presence of such structures casts doubt on the chaotic behavior of the considered mappings, because they clearly identify a stable structure.

CONCLUSIONS

As a result of the analysis of various approaches to the construction of pseudo-random sequences, it was established how the choice of initial conditions affects the structure of the sequence to be formed, namely: if the length of the period of the sequence corresponds to the dimension of the chosen prime number, then such a sequence is more similar to a chaotic one. On the contrary, it was found that under any circumstances, the existence of fixed points in the chosen nonlinear dynamical system does not lead to the creation of chaos, but on the contrary, unambiguously determines the existence of a stable structure with a fixed cycle length. The largest number of internal cycles is demonstrated by the sequences based on the mapping (1.5), it follows that the mapping (1.5) generates more deterministic sequences than other mappings considered.

If we talk about the applied significance of the above studies, in connection with the results of the work, it should be said that for reliable methods of generating pseudo-randomness, it is necessary to choose mappings that generate sequences with fewer similar internal structures and shorter length of these sequences, for their further combination and mixing.

LIST OF REFERENCES

1. Balasubramanian V., Ho S., Vovk V. Conformal Prediction for Reliable Machine Learning: Theory, Adaptations and Applications. – Elsevier, 2014. – 299 p.
2. Шарковский А.Н. Аттракторы Траекторий и их Басейны. Киев. Наукова Думка 2013, 319 с.
3. Wei-Bin Zhang. Synergetic Economics. Time and Change in Nonlinear Economics. – Springer Berlin, Heidelberg, 1991 – 246 p.
4. Rauch, J. Conjugating the tent and logistic maps. – Режим доступу до публікації: http://www.cs.ucr.edu/~eamonn/mapsconjugation.pdf
5. Hirsch, M., Smale, S. and Devaney, R. Differential equations, dynamical systems, and an introduction to chaos. Amsterdam: Academic Press. – 423 p.
6. Y. Manin., A. Panchishkin. Introduction to Modern Number Theory. –Springer Berlin, Heidelberg, 2005 – 514 p.
7. Успенский В.А. Четыре алгоритмических лица случайности. – М: МЦНМО, 2006. – 40 с.
8. H. Rogers. Theory of recursive functions and effective computability. – New York, McGraw-Hill, 1967 – 519 p.
9. Berndt, D., Clifford, J. Using Dynamic Time Warping to Find Patterns in Time Series. AAAI Press, 1994. – 359-370 p.
10. Vostrov G., Khrinenko A.,Kolisnichenko V. Behavior of fixed point periodic trajectories of nonlinear maps in dynamical systems theory , ISSN 2221-

3805.Електротехнічні та комп’ютерні системи, 32(108), 2020, UDC 519.216.1, p. 45-53

11. Lacasa L., Luque B., Gomes I., Miramontes O., On a Dynamical Approach to Some Prime Number Sequences, Entropy-20 00131, 2018, MDPI, Basel, Switzerland.
12. Vostrov G., Yakshyn I., Modeling of the primitive roots structure the are associated with given prime numbers. Journal Electrotechnic and Computer Systems , ISSN 2221-3805, Ministry of Education and Science of Ukraine, ONPU. 29(105), p. 171-176
13. Haken, H. Advanced Synergetics. – Berlin: Springer Berlin Heidelberg. – 1983. – 316 p.
14. M. Holodniok, A. Klíč, M. Kubíček, M. Marek. MMetody analýzy nelineárních dynamických modelů. – Praha : Academia. – 1986. – 424 s.
15. J. Nicolis. Dynamics of Hierarchical Systems. An Evolutionary Approach. – Springer Berlin Heidelberg, Berlin. – 1986. – 412 с.
16. Penrose, R. The Road to Reality: A Complete Guide to the Laws of the Universe. – Vintage. – 2007. – 1136 p.
17. Skiadas, Ch., Skiadas, Ch. Handbook of Applications of Chaos Theory. – CRC Press. – 2016. – 910 p.
18. Crandall R., Pomerance K. Prime numbers: cryptographic and computational aspects. – 2nd edition. – Springer, 2005. – 597 p.
19. Lynch, S. Dynamical Systems with Applications using Mathematica. – Birkhauser Boston. – 2007. – 477 p.

National University “Odessa Polytechnic”, Department Applied Mathematics and Information Technologies, Ukraine
Vostrov G. vostrov@gmail.com
Khrinenko A. khrinenko.andrew@gmail.com
Shcherbaniuk O. theotipax@gmail.com